**HYPOTHETICALS FOR FTC SAFEGUARDS DISCUSSION**

**Hypothetical 1:**

Jane Smith is an HR officer at Cheatum Motors in charge of recruiting. She received an email indicating it was from the President of Cheatum who asked her to log in to a website that detailed a sensitive dealership employee issue. When Jane clicked on the link, she viewed a page that was consistent with Cheatum’s website although a few words were misspelled. Clicking the website brought Jane to a landing page that required her to log in using her Cheatum user name and password. She entered both fields and received a message indicating her password was not recognized and asking her to log in again which she did, receiving the same error message. She attempted to log in a third time but gave up after she got the same error message.

Unbeknownst to Jane, the email was a well-designed phishing email that used Jane’s log in credentials to obtain and send a similar email from Jane to everyone on her contact list and in her hard drive. Jane possessed Social Security numbers on most Cheatum current and former employees as well as driver’s license numbers, email addresses, and credit reports on persons who had applied for jobs at Cheatum. Jane got phone calls and emails from long-lost employees thanking her for getting back in touch. Many asked Jane about the log-in request in the email. Jane had no knowledge of either the emails or the log-in request. She has come to you to seek your assistance.

You are the Chief Compliance Officer for Cheatum. Was this a security incident and, if so, what do you do next?

**Hypothetical 2:**

George works as a valet at Cheatum who is responsible for collecting name, address, and drivers license number of all customers who request a test drive or lease a rental vehicle. George has been seen spending an unusual amount of time at the copier. He brings a backpack to and from work each day and has a personal smartphone with a camera on it. Although George is a seven-year employee at Cheatum, he gives notice of his resignation telling his manager and HR that he wants to spend more time with his ailing mother who is 85 years old.

Six months later, the GM of Cheatum receives a call from the state Attorney General’s office. Facing an increase in identity theft cases and using a new AI program, the AG’s office looked for commonality among the victims’ credit reports, social media postings, and the time of their complaints. All of the complaints originated during the prior three-six months. About 75% of the victims had done business with Cheatum in the prior year. The AG has requested an audit of Cheatum’s Safeguards program, a general security audit of its procedures, and for a match of the victims’ name and personal data against customers of Cheatum and other consumers who provided personal information to Cheatum.

You are the Chief Compliance Officer for Cheatum. What do you do and how do you respond to the AG (besides telling them to get a subpoena)?

**Hypothetical 3:**

One of Cheatum’s competitors is Big Deal Motors. For several months, Cheatum has seen a decline in both online and in-store traffic. When salespeople at Cheatum have called prior customers, a surprising number of them have said they recently bought a vehicle from Big Deal. Big Deal outsources most of its IT work to Nerd & Co., a local IT company. Cheatum hires another IT company, Power On, to run an analysis of its system to meet its Safeguards requirements. Power On finds an unusual number of hits on Cheatum’s CRM system. An inordinate number of the hits have come from an IP address associated with Nerd & Co. On the hits from Nerd & Co’s IP address, Power On also determines that many of the hits appear to have had access to customer information as Cheatum has not encrypted the customer information because the FTC extended the date required to do so until June 9. Cheatum’s President calls Nerd & Co.’s President and indicates that there appear to be efforts to access its system from Nerd & Co.’s IP address. After conducting a preliminary investigation, Nerd & Co. finds no indication whatsoever of any Nerd & Co. employees or service providers accessing or attempting to access Cheatum’s system. He shares the results of this investigation with Cheatum’s President.

You are the Chief Compliance Officer for Cheatum. What are your next steps?